

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

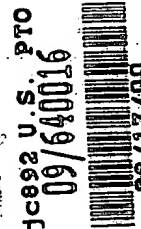
Applicant(s): Yasuhiko NAGAI, et al

Serial No.:

Filed: August 17, 2000

Title: SECURITY SYSTEM DESIGN SUPPORTING METHOD

Group:



LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

August 17, 2000

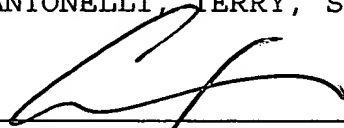
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 11-339304 filed November 30, 1999.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
\_\_\_\_\_  
Carl I. Brundidge  
Registration No. 29,621

CIB/nac  
Attachment  
(703) 312-6600

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JCE92 U.S. PTO  
09/640016  
08/17/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出願年月日  
Date of Application:

1999年11月30日

願番号  
Application Number:

平成11年特許願第339304号

願人  
Applicant(s):

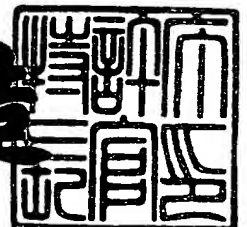
株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 7月28日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3059705

【書類名】 特許願

【整理番号】 K99014951

【提出日】 平成11年11月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 永井 康彦

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 藤山 達也

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 荒井 正人

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報システム事業部内

【氏名】 角田 光弘

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報システム事業部内

【氏名】 山田 知明

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティシステム設計支援方法

【特許請求の範囲】

【請求項 1】

情報関連製品や情報システムの計画／設計段階での国際セキュリティ評価基準に基づくセキュリティ要求仕様書やセキュリティ設計仕様書の設計支援をおこなうセキュリティシステム設計支援方法において、

国際登録された P P 群あるいは過去に作成された国際登録外の P P / S T 群を P P / S T 群が対象とする製品・システム種別間の継承関係に基きクラスツリー構造化して格納した雛型事例データベースを設け、

設計対象の構成要素・種別・認証レベル指定により、設計対象に関する P P / S T 群をツリー検索して特定し、

特定 P P / S T 群の定義内容を統合編集して設計対象の P P / S T 原案を自動生成する

ことを特徴とするセキュリティシステム設計支援方法。

【請求項 2】

P P / S T 構築事例より蓄積した製品・システムの構成要素と対応するセキュリティ環境（前提、脅威、組織のポリシー）と、セキュリティ環境と対応するセキュリティ目標と、セキュリティ目標と対応するセキュリティ評価基準と、セキュリティ評価基準と対応する実現方式の対応情報を格納した部分事例データベースを設け、

構成要素と、セキュリティ環境と、セキュリティ目標と、セキュリティ評価基準との指定により各々対応する対応情報へ自動変換し、

設計対象の P P / S T の定義内容の部分を自動生成することを特徴とするセキュリティシステム設計支援方法。

【請求項 3】

請求項 1 記載のセキュリティシステム設計支援方法により P P / S T 原案を自動生成し、請求項 2 記載のセキュリティシステム設計支援方法により P P / S T の部分追加・修正することを特徴とするセキュリティシステム設計支援方法。

【請求項 4】

請求項 1 記載のセキュリティシステム設計支援方法において、

雛型事例データベースに格納されている PP/ST 群を構成要素・種別・認証レベルが識別可能なアイコンとして表現し、

PP/ST 間の継承関係をツリー図表現した参照 PP/ST 事例表示から、設計対象と関連性がある PP/ST 群を継承ツリーから特定可能とし、

特定された PP/ST 群のアイコンを構成要素として設計対象の構成図を作成する

ことを特徴とするセキュリティシステム設計支援方法。

【請求項 5】

請求項 2 記載のセキュリティシステム設計支援方法において、

部分事例データベースに各脅威の発生確率と影響損失額データと、各セキュリティ目標の対策コストデータとを合わせて格納・蓄積し、

各脅威のリスク（発生確率×影響損失額）と対応セキュリティ目標群の対策コストの関係に対し、リスク許容値、コスト制限値、残存リスク／対策コスト比率の制約条件とコスト最小化あるいは対策リスク最大化の評価関数を指定して組み合わせ最適化問題を定式化し、

前記最適化問題を求解することで投資効果のある最適なセキュリティ目標を決定する

ことを特徴とするセキュリティシステム設計支援方法。

【請求項 6】

請求項 2 記載のセキュリティシステム設計支援方法において、

自動生成された定義内容の要件が、基準規定の機能要件及び保証要件間の依存関係や階層関係と整合するか否かを基準規定の依存・階層関係を基に検証することを特徴とするセキュリティシステム設計支援方法。

【請求項 7】

請求項 1 ないし 3 いずれかに記載のセキュリティシステム設計支援方法において、

定義されたセキュリティ環境や、セキュリティ目標や、セキュリティ基準や、

実現方式またはそれら各々の間の対応関係から P P / S T の定義内容の一部である各対応関係をマトリックス表で表現した根拠マトリックスを自動生成し、

対応抜け定義情報の有無を検証する

ことを特徴とするセキュリティシステム設計支援方法。

【請求項 8】

請求項 1 ないし 3 いずれかに記載のセキュリティシステム設計支援方法において、

P P / S T 作成過程での新規追加情報や P P / S T 作成結果を、雛型事例データベースや部分事例データベースの継承関係や対応関係に従い格納し、

事例データベースの格納情報の充実・拡張を行う

ことを特徴とするセキュリティシステム設計支援方法。

【請求項 9】

請求項 1 ないし 3 いずれかに記載のセキュリティシステム設計支援方法において、

作成された P P / S T を国際セキュリティ評価方法に準拠した問診表形式の P P / S T 評価チェックリストを表示し、評価可能にする

ことを特徴とするセキュリティシステム設計支援方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報システムや製品の計画・設計段階における、システムや製品のセキュリティ施策を設計するためのセキュリティシステム設計支援方法とその方法に基づく設計支援ツールに関するものである。

【0 0 0 2】

【従来の技術】

I S O 1 5 4 0 8 として国際標準化されたセキュリティ評価基準コモンクライテリア(Common Criteria, 以下 C C と呼ぶ)は、情報システムや製品に必要となる基本的なセキュリティ機能要件とその機能品質の保証要件、および 7 段階の保証レベルを規定している。

【0003】

ユーザー情報部門担当者や製品開発者、システム設計／構築を行うSE(System Engineer)は、このCC規定要件から自身の対象製品・システムに必要な要件を選択してセキュリティ要求仕様書（プロテクション・プロファイル、以下PPと呼ぶ）やセキュリティ基本設計書（セキュリティ・ターゲット、以下STと呼ぶ）を作成し、開発・構築を行うこととなる。

【0004】

また、この基準に基づく評価・認証制度が確立され、設定した保証レベルに対応する評価・認証を指定の評価・認証機関から取得することとなる。

【0005】

標準化以降、あらゆる情報関連製品・システムは、このCC準拠での構築、評価・認証取得が顧客調達要件、ネットワーク接続要件、システム運用条件、法制度や業界制度として活用され、認証取得が必須の条件となる。

【0006】

そこで、認証取得のために計画／設計段階にて作成することが必須となるPP／STの作成作業を支援するための作成ガイドや支援ツールが開発されている。

【0007】

PPやST仕様書の各章で記述すべき項目や表記形式と事例サンプルを提示することでPP／STの形式化を支援する技術が、文献アイ・エス・オー/エス・シー・27、エヌ・2333、ガイド・フォー・プロダクション・オブ・プロテクションプロファイルズ・アンド・セキュリティターゲットズ、第0.8版（1999年7月）（ISO/SC27 N2333 Guide for Production of Protection Profiles and Security Targets Version 0.8, July, 1999）や文献情報技術セキュリティ評価基準ISO/IEC 15408セミナー資料集（1999年9月8日情報処理振興事業協会セキュリティセンター主催）第26頁から第33頁に記載されている。

【0008】

【発明が解決しようとする課題】

しかしながら、上記従来のCC準拠のセキュリティ設計支援技術は、基本的にPP／STの仕様書形式の整合のみを支援するものであったり、内容情報の導出



・定義支援技術も対象製品やシステム毎に毎回ゼロから作成する必要があるものである。

このため、PP/STの形式調整や記述内容を手続き的に抽出・定義することはできるが、作成者に対し、CCやセキュリティ脅威・対策に関する専門知識やノウハウ、リスク分析の専門技術が要求され、膨大な作業工数がかかること、また、作成PP/STの品質が作成者のこれら知識や能力に依存し均一化が図れないという問題があった。

#### 【0009】

さらに、PPは本来同種の製品・システム設計において再利用、共有されるべきものであり、作成されたPPの中で指定の評価機関で評価合格し、指定PP登録機関に登録されたPPは、登録PPが対象とする製品・システムと同種のものを設計する場合、登録PPを基本的に活用することが必要となる。

しかし、上記従来のCC準拠のセキュリティ設計支援技術では、登録PPや過去作成事例を再利用することを支援するものではないという問題もあった。

#### 【0010】

本発明は、登録PPや過去のST作成事例やその部分を雛型や部品として再利用あるいは参照情報として有効活用し、CCや脅威・対策、リスク分析の専門知識・ノウハウや技術を持たない設計者でもPP/STの作成を可能とし、かつ作成工数の効率化や作成品質の均一化が図れるCC準拠のセキュリティシステム設計支援方法及び本方法に基づく支援ツールを提供することを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

上記の目的を達成するために、本発明によるセキュリティシステム設計支援ツール及び方法では、以下のDBを設ける。

・登録PP及びPPファミリーの各PPをオブジェクト指向デザインのオブジェクトクラスとして捉えた事例／ノウハウDB(Data Base)。ファミリーとは、同じセキュリティ目標を持つがCC機能要件コンポーネントや保証要件コンポーネントが異なる複数のPP群を指す。

・PP間のクラス継承関係に基づきクラスツリー構造で各PPを格納した登録P

P/PPファミリーツリー構造化DBや、CC要件コンポーネントやCEM(Common Evaluation Methodology: CC準拠の標準評価手法)評価コンポーネント及び登録パッケージを、標準規定のクラス・ファミリー・コンポーネント間およびコンポーネント間の階層構造に従い格納したCC(CEM)/PKG構造化DBからなる標準登録事例・情報活用のためのDB群。パッケージとは、再利用の目的で定義された機能及び保証コンポーネントの組合せであり、PPまで構成しない部分的、中間的纏まりのことで、以下ではPKGと呼ぶ。

- ・標準登録外の既存PP/STも上記と同様PP/ST間のクラス継承関係に基づきクラスツリー構造で各PP/STを格納したローカルPP/STツリー構造化DB。

- ・標準登録されていないため独自で追加拡張定義したCC要件コンポーネントやPKGを格納した拡張CC/PKG構造化DBからなる標準登録外ローカル事例・情報活用のためのDB群。

#### 【0012】

- ・過去のPP/ST作成事例の部分事例として、設計対象製品・システムの構成要素群に関連する脅威（発生確率データ含む）／前提／組織ポリシー群の対応事例部品、各脅威／前提／組織ポリシーに関連するセキュリティ目標群（対策コスト／リスク許容値データ含む）の対応事例部品や、セキュリティ目標群に関連するCC要件コンポーネント群の対応事例部品や、CC要件コンポーネント群に関連する実現方式群の対応事例部品からなる対応ノウハウDB。

#### 【0013】

次に、これら登録及び登録外事例DBや対応ノウハウDBの格納情報を利用してPP/STを準自動作成支援する手段として以下を設ける。

- ・設計対象製品・システムの構成要素、種別、要求認証レベルを登録PP/PPファミリーツリー構造化DBとローカルPP/STツリー構造化DBに格納されているPP/ST群に対応したアイコン群をクラスツリー構造で表示した画面上で該当あるいは属するアイコンを選択指定すると関連するPP/STを自動検索し、各章別に統合編集して設計対象のPP/STの雛型を自動生成する手段。

- ・自動生成されたPP/ST原案の第3章セキュリティ環境における前提条件、

脅威、組織のセキュリティポリシーの定義情報を対応ノウハウDB情報を参照して追加・修正する追加環境定義手段。

・追加・修正されたセキュリティ環境情報に対応するセキュリティ目標へ対応ノウハウDB情報を参照して自動変換して原案の4章セキュリティ目標に追加・修正する環境→目標変換手段。

【0014】

・3章で定義された各脅威のリスク値（脅威の発生確率×影響の大きさ）と4章に定義されている各セキュリティ目標の実施コストを対応ノウハウDB参照または演算支援により設定、目標最適化の制約条件（リスク許容値、コスト制限値、リスク対コスト比率）及び評価関数（コスト最小化関数、対策リスク最大化関数）を対話的に選択・設定して設定条件下での組み合わせ最適化問題を求解することで設定条件下での最適セキュリティ目標の組み合わせを決定し、決定目標に基づき3章の脅威および4章の脅威対応セキュリティ目標を修正する手段。

・4章で決定したセキュリティ目標群に対応するCC要件コンポーネント群をCC(CEM)/PKG構造化DB、拡張CC/PKG構造化DBおよび対応ノウハウDB参照により自動変換して5章セキュリティ要件を定義する手段。

・ST作成の場合は、さらに5章セキュリティ要件の定義CC要件コンポーネント群に対応する実現方式群を対応ノウハウDB参照により自動変換して6章対象システムの仕様概要の内容として定義する手段。

・2章以降定義された環境－目標－CC要件－実現方式の各項目間の対応関係（PP作成の場合はCC要件まで）を表現した根拠マトリックス表を自動生成および未対応項目の有無を検証し8章根拠の内容として定義する手段。

・最後に以上の手段で作成されたPP/STをCC(CEM)/PKG構造化DBに格納されたCC保証要件やCEMのPP/ST評価項目情報をチェックリスト形式で表示し、対話的に作成したPP/STを簡易評価する手段。

【0015】

すなわち、本発明によるセキュリティシステム設計支援方法は、情報関連製品や情報システムの計画／設計段階での国際セキュリティ評価基準に基づくセキュリティ要求仕様書やセキュリティ設計仕様書の設計支援をおこなうセキュリティ

システム設計支援方法において、国際登録されたPP群あるいは過去に作成された国際登録外のPP/ST群をPP/ST群が対象とする製品・システム種別間の継承関係に基づきクラスツリー構造化して格納した雛型事例データベースを設け、設計対象の構成要素・種別・認証レベル指定により、設計対象に関するPP/ST群をツリー検索して特定し、特定PP/ST群の定義内容を統合編集して設計対象のPP/ST原案を自動生成することを特徴とする。

## 【0016】

また、本発明は、PP/ST構築事例より蓄積した製品・システムの構成要素と対応するセキュリティ環境（前提、脅威、組織のポリシー）と、セキュリティ環境と対応するセキュリティ目標と、セキュリティ目標と対応するセキュリティ評価基準と、セキュリティ評価基準と対応する実現方式の対応情報を格納した部分事例データベースを設け、構成要素と、セキュリティ環境と、セキュリティ目標と、セキュリティ評価基準との指定により各々対応する対応情報へ自動変換し、設計対象のPP/STの定義内容の部分を自動生成することを特徴とする。

## 【0017】

さらに、これらのセキュリティシステム設計支援方法を用い、自動生成したPP/ST原案に、部分追加・修正していくことを特徴とする。

また、雛型事例データベースに格納されているPP/ST群を構成要素・種別・認証レベルが識別可能なアイコンとして表現し、PP/ST間の継承関係をツリー図表現した参照PP/ST事例表示から、設計対象と関連性があるPP/ST群を継承ツリーから特定可能とし、特定されたPP/ST群のアイコンを構成要素として設計対象の構成図を作成することを特徴とする。

また、定義内容の統合編集において、国際登録PPからの定義内容と過去作成の国際登録外PP/STからの定義内容とを文字フォント、文字スタイル、文字サイズや色別により識別できるようにすることを特徴とする。

## 【0018】

また、部分事例データベースに各脅威の発生確率と影響損失額データと、各セキュリティ目標の対策コストデータとを合わせて格納・蓄積し、各脅威のリスク（発生確率×影響損失額）と対応セキュリティ目標群の対策コストの関係に対し

、リスク許容値、コスト制限値、残存リスク／対策コスト比率の制約条件とコスト最小化あるいは対策リスク最大化の評価関数を指定して組合わせ最適化問題を定式化し、前記最適化問題を求解することで投資効果のある最適なセキュリティ目標を決定することを特徴とする。

また、自動生成された定義内容の要件が、基準規定の機能要件及び保証要件間の依存関係や階層関係と整合するか否かを基準規定の依存・階層関係を基に検証することを特徴とする。

#### 【0019】

また、定義されたセキュリティ環境や、セキュリティ目標や、セキュリティ基準や、実現方式またはそれら各々の間の対応関係からPP／STの定義内容の一部である各対応関係をマトリックス表で表現した根拠マトリックスを自動生成し、対応抜け定義情報の有無を検証することを特徴とする。

また、PP／ST作成過程での新規追加情報やPP／ST作成結果を、雛型事例データベースや部分事例データベースの継承関係や対応関係に従い格納し、事例データベースの格納情報の充実・拡張を行うことを特徴とする。

また、作成されたPP／STを国際セキュリティ評価方法に準拠した問診表形式のPP／ST評価チェックリストを表示し、評価可能にすることを特徴とする。

#### 【0020】

また、本発明によるセキュリティシステム設計支援ツールは、

事例／ノウハウデータベースとして、登録PP及びPPファミリーをPP間のクラス継承関係に基づきツリー構造で格納した登録PP／PPファミリーツリー構造化データベースと、セキュリティ基準の要件コンポーネントやセキュリティ評価手法の評価コンポーネント及び登録パッケージを標準規定のクラス・ファミリー・コンポーネント間およびコンポーネント間の階層構造に従い格納した標準情報構造化データベースとを標準登録事例・情報活用のためのデータベース群として設け、

標準登録外の既存PP／STを上記と同様PP／ST間のクラス継承関係に基づきツリー構造で格納したローカルPP／STツリー構造化データベースと、標

準登録されていないため独自で追加拡張定義したセキュリティ要件コンポーネントやパッケージを格納した拡張標準情報構造化データベースとを標準登録外ローカル事例・情報活用のためのデータベース群として設け、

さらに、過去のPP/ST作成事例の部分事例として、設計対象製品・システムの構成要素群に関連する脅威（発生確率・影響損失データ含む）／前提／組織ポリシー群の対応事例部品と、各脅威／前提／組織ポリシーに関連するセキュリティ目標群（対策コストデータ含む）の対応事例部品と、セキュリティ目標群に関連するセキュリティ要件コンポーネント群の対応事例部品と、セキュリティ要件コンポーネント群に関連する実現方式群の対応事例部品とを対応ノウハウデータベースとして設ける。

#### 【0021】

さらに、これら事例／対応ノウハウデータベースの格納情報を利用してPP/STを準自動作成支援する手段として、

設計対象製品・システムの構成要素、種別、要求認証レベルを登録PP/PPファミリーツリー構造化データベースとローカルPP/STツリー構造化データベースに格納されているPP/ST群に対応したアイコン群をクラスツリー構造で表示した画面上で該当あるいは属するアイコンを選択指定すると関連するPP/STを自動検索し、各章別に統合編集して設計対象のPP/STの雛型を自動生成する手段と、

自動生成されたPP/ST原案の第3章セキュリティ環境における前提条件、脅威、組織のセキュリティポリシーの定義情報を対応ノウハウデータベース情報を参照して追加・修正する追加環境定義手段と、

追加・修正されたセキュリティ環境情報に対応するセキュリティ目標へ対応ノウハウデータベース情報を参照して自動変換して原案の4章セキュリティ目標に追加・修正する環境→目標変換手段と、

3章で定義された各脅威のリスク値（脅威の発生確率×影響損失額）と4章に定義されている各セキュリティ目標の対策コストを対応ノウハウデータベース参照または演算支援により設定、目標最適化の制約条件（リスク許容値、コスト制限値、リスク対コスト比率）及び評価関数（コスト最小化関数、対策リスク最大

化関数) を対話的に選択・設定して設定条件下での組合わせ最適化問題を求解することで設定条件下での最適セキュリティ目標の組合わせを決定し、決定目標に基づき 3 章の脅威および 4 章の脅威対応セキュリティ目標を修正する手段と、

4 章で決定したセキュリティ目標群に対応するセキュリティ要件コンポーネント群を標準情報構造化データベース、拡張標準情報構造化データベースおよび対応ノウハウデータベース参照により自動変換して 5 章セキュリティ要件を定義する手段と、

ST 作成の場合は、さらに 5 章セキュリティ要件の定義要件コンポーネント群に対応する実現方式群を対応ノウハウデータベース参照により自動変換して 6 章対象システムの仕様概要の内容として定義する手段と、

2 章以降定義された環境－目標－セキュリティ要件－実現方式の各項目間の対応関係を表現した根拠マトリックス表を自動生成および未対応項目の有無を検証し 8 章根拠の内容として定義する手段と、

作成された PP/ST を標準情報構造化データベースに格納された保証要件やセキュリティ評価方法の PP/ST 評価項目情報をチェックリスト形式で表示し、対話的に作成した PP/ST を簡易評価する手段とを設けたことを特徴とする。

#### 【 0 0 2 2 】

また、上記セキュリティシステム設計支援ツールのデータベース群及び各手段を設計支援サービスサーバに設け、利用者クライアントが設計支援サービスサーバにネットワーク接続して手段をダウンロードし、共用データベースにアクセスして利用できることを特徴とする。

また、上記設計支援サービスサーバを異なる組織毎に複数設け、サーバ内の分散データベースリンク手段により、複数組織の事例/ノウハウ DB をネットワークを介して仮想的な統一データベースとして利用できるセキュリティシステム設計支援サービスの提供を特徴とする。

#### 【 0 0 2 3 】

また、上記設計支援サービスサーバを民間機関に設け、国内登録や業界登録 P/P ファミリーツリー構造化データベースや、ローカル PP/ST ツリー構

造化データベースや、拡張標準情報構造化データベースを格納した基準提供サーバを国内標準機関あるいは特定業界機関に設け、国際登録PP/PPファミリーツリー構造化データベースや、標準情報構造化データベースを格納した国際基準提供サーバを国際PP登録機関に設け、さらに民間機関設計支援サービスサーバ内に国際機関、国内あるいは業界機関サーバの情報更新を監視し、更新検知時には民間機関サーバへ最新情報をダウンロードする情報更新監視制御手段を設け、国際機関、国内機関の階層レベルや適用業界分野特化の異なる事例情報をネットワークを介して利用できることを特徴とする。

## 【0024】

## 【発明の実施の形態】

以下、本発明の実施形態について図面を用いて説明する。

第一実施例としてスタンドアローン型のセキュリティシステム設計支援ツールでPP/ST仕様書を作成する場合の構成・動作について説明する。

図1は、本発明によるセキュリティシステム設計支援ツールの特徴概要図である。

## 【0025】

本ツールは、規定形式のPP/ST仕様書101の作成支援のために、登録PP/PPファミリーツリー構造化DBとCC(CEM)/PKG構造化DBの標準規定・登録事例情報と、ローカルPP/STツリー構造化DBと拡張CC/PKG構造化DBおよび対応ノウハウDBといった過去のPP/ST作成結果として得られる標準登録外のローカル事例部品情報を再利用、有効活用する事例/ノウハウDB102と、新規設計対象のPP/ST原案を自動生成し、その原案を対話的に追加・修正支援するPP/ST準自動生成機能103を有している。

## 【0026】

図2は本発明によるセキュリティシステム設計支援ツールの構成図である。

本発明によるセキュリティシステム設計支援ツール225は、データベース206、プログラムメモリ219、定義画面や評価結果表示画面を表示するCRT220、PP/ST編集入力や関連情報を選択・設定するためのキーボード221、マウス222及びこれら入出力を制御する入出力制御部223、さらに入出



力、メモリ、データベースへのアクセスや各プログラムを実行するCPU224から構成される。

#### 【0027】

データベース206は、登録PP及びPPファミリーを各PPをオブジェクト指向デザインのオブジェクトクラスとして捉え、PP間のクラス継承関係に基づきクラスツリー構造で各PPを格納した登録PP/PPファミリーツリー構造化DB201と、CC要件コンポーネントやCEM評価コンポーネント及び登録パッケージを標準規定のクラス・ファミリー・コンポーネント間およびコンポーネント間の階層構造に従い格納したCC(CEM)/PKG構造化DB202と、標準登録外の既存PP/STも上記と同様PP/ST間のクラス継承関係に基づきクラスツリー構造で各PP/STを格納したローカルPP/STツリー構造化DB203と、標準登録されていないため独自で追加拡張定義したCC要件コンポーネントやPKGを格納した拡張CC/PKG構造化DB204と、過去のPP/ST作成事例の部分事例として、設計対象製品・システムの構成要素群に関連する脅威（発生確率／リスクデータ含む）／前提／組織ポリシー群の対応事例部品、各脅威／前提／組織ポリシーに関連するセキュリティ目標群（対策コスト／リスク許容値データ含む）の対応事例部品、セキュリティ目標群に関連するCC要件コンポーネント群の対応事例部品、CC要件コンポーネント群に関連する実現方式群の対応事例部品を格納した対応ノウハウDB205とからなる。

#### 【0028】

また、プログラムメモリ219には、データベース206の情報検索・登録を制御する事例・ノウハウ情報管理制御部208、PP/STドキュメント編集処理部209、構成要素→参照PP自動検索・統合編集出力処理部210、追加環境定義支援処理部211、環境→目標変換処理部212、最適目標決定処理部213、目標→CC要件変換処理部214、CC要件→実現方式変換処理部215、根拠マトリックス生成・検証処理部216、PP/ST簡易評価処理部217、PP/STドキュメントの定義・編集・表示処理の制御をする定義／表示制御部218が格納されている。

## 【0029】

次に、本発明に係るセキュリティシステム設計支援ツールにおいてPP/ST作成処理をする場合の動作の一例を図1～図9を用いて説明する。

図3、図4は本発明の設計支援ツールを利用したPP/ST作成処理の動作フロー図である。以下、順を追って説明する。

## 【0030】

ステップ301：

利用者は図5に示すCRT220上の設計支援ツールのデータベース206の登録PP/PPファミリー構造化DB201、ローカルPP/STツリー構造化DB203を検索して初期画面上表示されるPP/STテンプレート選択ダイアログ401において、PP/ST間の継承関係を表現したツリー形式で参照表示される標準登録及びローカル登録PP/ST部品アイコン402を構成要素としてマウス222により選択、ドラッグ&ドロップ操作で設計対象製品・システムの構成図403を作成する。

## 【0031】

登録PP/PPファミリー構造化DB201、ローカルPP/STツリー構造化DBには、過去に登録・作成されたPP/STがPP/ST間の継承ツリー関係に基づいて上位PP/STをポインターでリンクしたテーブル構造で格納されており、各テーブルには各PP/STの表紙に記載されたPP名称、バージョン情報、発行日から成るPP/ST識別名、認証レベル、PP/STドキュメントファイルが登録されている。

## 【0032】

PP/ST部品アイコン402は、この識別名のPP/ST名称と認証レベル情報を用いて表現され、ツリー形式表示は、上位PP/STポインターリンクを利用して表現される。

## 【0033】

設計対象の構成図作成において、設計対象の構成要素と一致する要素がない場合は、ツリー表現の継承関係を参考に上位の概念の要素で最も近い要素があれば、それを選択する。

【0034】

図5のように認証レベル4（EAL4）のICカードシステムを設計対象とする場合、登録PPテンプレートから構成要素としてEAL4のICカードPP404、ICカードリーダー/ライター（R/W）PP405を選択、ローカルPPテンプレートからEAL4の本人認証端末PP406を構成要素として選択することとなる。

【0035】

ステップ302：

構成図作成後、テンプレートダイアログの設定ボタン407を押下すると選択構成要素のPP/ST群を構成要素→参照PP自動検索・統合編集出力処理部210が事例・ノウハウ情報管理制御部208を介してデータベース206の登録PP/PPファミリー構造化DB201、ローカルPP/STツリー構造化DBを検索して選択されたPP/STの各章の定義情報を複写・統合編集し、定義/表示制御部218により図6のようなPP/STドキュメント編集画面501上出力表示する。

【0036】

登録PPより抽出した定義情報はボールド文字表示502、ローカルPP/STより抽出した定義情報は普通文字表示503により登録情報とローカル情報を識別表示する。これは登録PP情報を参照した場合、参照情報内容に変更不可であり、そのまま利用する必要があることからその識別を容易にするためである。

【0037】

また、7章利用PP宣言には登録PPとして選択したものの中のPP識別名（PP名称、バージョン情報、発行日）504を編集・定義する。

【0038】

これにより、既存PP/ST事例を雛型として設計対象に関するPP/ST原案が自動生成されたこととなる。

【0039】

ステップ303：

出力されたPP/ST原案に対して1～3章の定義内容をドキュメント編集処

理部 2 0 9 により対話的に追加・修正するとともに追加構成要素に対しては、ツールメニュー 6 0 1 の追加環境定義支援 6 0 2 を選択、追加環境定義支援処理部 2 1 1 により対応ノウハウ DB 2 0 5 の図 8 に示すような構成要素—環境対応表 7 0 1 の構成要素を参照して表示される追加構成要素候補リストダイアログより追加要素を選択（候補リストにない場合は、新規構成要素としてキーボード 2 2 1 より新規要素とその対応環境情報定義入力）、設定ボタン押下により構成要素—環境対応表 7 0 1 から該当構成要素→脅威／前提／組織ポリシー対応事例部品を検索して 3 章セキュリティ環境の定義内容も追加定義する。

【 0 0 4 0 】

ステップ 3 0 4 :

ツールメニュー 6 0 1 の環境→目標変換 6 0 3 選択により、環境→目標変換処理部 2 1 2 が 3 章の定義内容である脅威／前提／組織ポリシーを対応ノウハウ DB 2 0 5 の環境—目標対応表 7 0 2 検索によりセキュリティ目標に変換し、4 章の既定義目標との差分を追加定義する。

【 0 0 4 1 】

ここで、環境—目標対応表 7 0 2 の各脅威に対抗する目標は、脅威を起こさないために防止すべき必要十分な要因に対応する対策目標の組合わせ（ミニマルパスセット；例えば、図 8 の 7 0 3 の各括弧要素が各々対策目標案で、この場合 2 つの内の一方で脅威対抗が可能）が格納されている。また複数の脅威に対して同じ対策目標が対応する可能性もある。

【 0 0 4 2 】

なお、DB 上存在しない新規環境の場合は新規環境—目標対応入力ダイアログが表示されキーボード 2 2 1 で対応目標を入力し環境—目標対応表 7 0 2 に追加格納する。

【 0 0 4 3 】

その際、新規脅威の対応目標定義は、従来技術である F T A (Fault Tree Analysis) ツールと連動して、脅威を頂上事象とする F T を作成して頂上事象に関する基本事象（要因）を特定し、ミニマルパスセット演算によりミニマルパスセットとなる基本事象の組合わせを求め、各セット毎の基本事象に対抗する対策目標

を定義することで脅威対抗の対策目標の組合わせを導出して追加格納する。

【0044】

ステップ305:

ツールメニュー601の最適目標決定604のデータ設定605を選択、最適目標決定処理部213により対応ノウハウDB205の脅威データ表704、対策コストデータ表705検索でダイアログ表示される3章定義脅威の発生確率、影響損失額、4章セキュリティ目標の対策コスト値を確認し、データ未設定である新規脅威や新規目標のデータを対話的に追加設定する。

【0045】

その際、新規脅威分の発生確率データは、先の対応目標定義で利用したFTAツールと再連動して、作成した該当脅威を頂上事象とするFTの基本事象の発生確率を入力し、頂上事象の発生確率導出演算を実行することにより解析的に求めて設定する。

【0046】

ステップ306:

ツールメニュー601の最適目標決定604の目標最適化演算606を選択、最適目標決定処理部213により図9のようにダイアログ表示801される制約条件803、評価関数802を設定、実行ボタン押下804により対応ノウハウDB205の脅威データ表704、対策コストデータ表705検索で演算実行し、最適解となるセキュリティ目標の組合わせと対応する脅威を基に3章脅威、4章目標の定義内容を自動修正する。

【0047】

評価関数802は、セキュリティ目標の対策コストを最小化するコスト最小化関数と、目標により対策する脅威のリスク（脅威発生確率×影響損失額）の総和を最大化する対策リスク最大化関数のいずれか一方を選択、制約条件803は、指定値以下のリスクの脅威を許容できるものとして対策から除外するリスク許容値、対策コストの総和を指定値以下に押さえるコスト制限値、対策されない残存脅威のリスク総和と対策コスト総和の比率で残存損失額と対策費用の投資効果点（比率1で残存損失と対策費用の総和が最小となる）を指定するリスク対コスト

比率の中から一つ以上を選択する。

【0048】

最適化演算をする際、更新前の3章、4章において登録PPより参照された脅威およびその脅威対抗の目標がある場合、それらの採用を最適化問題の制約条件に含めて演算する。

これは登録PPを参照して新規PP/STを作成する場合、登録PPの定義内容の削減は許されないからである。

ただし、その登録PPを参照PPから削除しても良い場合は、最適化問題の制約条件に含める必要はない代わりに7章利用PP宣言の記述から該当登録PP識別名を削除する。

この選択は最適化演算前に登録PP参照解除可否のメッセージ通知により対話的に設定する。

【0049】

上記最適目標決定演算は、設定された評価関数と制約条件を反映したセキュリティ目標の組合わせ最適化問題を求解する演算となる。

例えば、3章の脅威として、T-1（発生確率；0.1,影響損失額；100000000円,リスク値；10000000円）、T-2（発生確率；0.1,影響損失額；50000000円,リスク値；5000000円）、T-3（発生確率；0.2,影響損失額；5000000円,リスク値；1000000円）、T-4（発生確率；0.01,影響損失額；10000000円,リスク値；100000円）であり、4章の目標として、O-1（対策コスト；1000000円）、O-2（対策コスト；100000円）、O-3（対策コスト；200000円）、O-4（対策コスト；300000円）、O-5（対策コスト；200000円）、O-6（対策コスト；150000円）、O-7（対策コスト；400000円）、O-8（対策コスト；600000円）、O-9（対策コスト；1000000円）、O-10（対策コスト；800000円）が挙げられ、T-1に対する目標組合わせが（O-1, O-2）（O-3）、T-2に対する目標組合わせが（O-4, O-6）（O-1, O-5）、T-3に対する目標組合わせが（O-2, O-3）（O-7）、T-4に対する目標組合わせが（O-8, O-9）（O-10）であるとする。

【0 0 5 0】

この場合、評価関数としてコスト最小化関数、制約条件としてリスク許容値＝100000円を設定して最適目標決定演算を実行すると、まずリスク許容値＝100000円より脅威T－4がリスク値＝100000円のため対象から削除、これにともないT－4の対応目標O－8，O－9，O－10も他の脅威と関連しないため対象から削除される。

従って、残りのT－1～T－3の脅威を最小のコストで対策できるO－1～O－7の組合わせを求める最適化問題となり、以下に示す最適化の評価関数式と、

【0 0 5 1】

【数1】

$$\text{Minimize : } Z = \sum_{a=1}^m C(q) \cdot \text{obj}(q) \quad \dots (\text{数1})$$

【0 0 5 2】

以下に示す最適化の制約条件式、

【0 0 5 3】

【数2】

$$1 - \sum_{k=1}^n \prod_{j=1}^{p_k} \text{obj}(q) = 0 \quad \dots (\text{数2})$$

【0 0 5 4】

【数3】

$$\text{obj}(q) \in \{1, 0\}, \quad (1 ; \text{採用}, 0 ; \text{否採用}) \quad \dots (\text{数3})$$

【0 0 5 5】

との組合わせ最適化問題として定式化される。

【0056】

評価関数式はコスト最小となる目標を選択することを表現し、前者の最適化の制約条件式は選択目標の組合わせで対象脅威が全て対策されるという条件式、後者の最適化の制約条件式は、目標  $q$  の採否を表現する条件式である。

【0057】

ここで、 $C(q)$  は目標  $q$  の対策コスト、 $m$  は対策目標候補数、 $obj(q)$  は目標候補  $q$  を採用するか否かの指示変数、 $n$  は対象脅威数、 $p_k$  は脅威  $k$  の目標組合わせ数、 $P_{k,j}$  は脅威  $k$  の  $j$  番目の目標組合わせを示す。

【0058】

先の例の場合の最適化問題を間接列挙法などの求解方法により演算すると、最適解：採用目標  $O-2$ ， $O-3$ ， $O-4$ ， $O-6$  の時、対策コスト最小値：750000円が求められる。

$T-1$  に対する目標として  $O-3$ ， $T-2$  に対する目標として  $O-4$ ， $O-6$ ， $T-3$  に対する目標として  $O-2$ ， $O-3$  が対応づけられる。

従って、3章の脅威として  $T-1 \sim T-3$  が決定し、4章の目標として  $O-2$ ， $O-3$ ， $O-4$ ， $O-6$  が決定され、各々3章、4章の定義内容を更新することとなる。

【0059】

ステップ 307：

ツールメニュー 601 の目標  $\rightarrow$  CC要件変換 607 を選択してダイアログ表示される EAL レベル設定により、目標  $\rightarrow$  CC要件変換処理部 214 が、対応ノウハウ DB 205 の目標  $\rightarrow$  CC要件対応表 706 を検索して4章目標に対応する CC機能要件を特定、また CC/PKG 構造化 DB 202，拡張 CC/PKG 構造化 DB 204 を検索し指定 EAL レベルの CC保証要件を特定して5章のセキュリティ要件の定義内容を自動修正する。

自動修正した結果は、CC/PKG 構造化 DB 202 の CC 情報に規定された CC要件間の依存関係や階層関係との論理的整合を検証し、不整合点はメッセージ通知して対話的な修正を促す。



【 0 0 6 0 】

定義内容の修正において、修正前の 5 章要件定義の登録 P P からの参照要件が削除対象となる時、登録 P P 参照を活かす場合は、削除せずに残し、その登録 P P を参照 P P から削除しても良い場合は 7 章利用 P P 宣言の記述から該当登録 P P 識別名を削除する。

この選択は自動修正前に登録 P P 参照解除可否のメッセージ通知により対話的に設定する。

【 0 0 6 1 】

ステップ 3 0 8 :

S T 作成の場合、ツールメニュー 6 0 1 の C C 要件→実現方式変換 6 0 8 選択により、C C 要件→実現方式変換処理部 2 1 5 が対応ノウハウ D B 2 0 5 の C C 要件—実現方式対応表 7 0 7 を検索し、5 章定義 C C 機能要件に対応する実現方式を特定して 6 章のシステム仕様概要の定義内容として設定する。

【 0 0 6 2 】

ステップ 3 0 9 :

ただし、既存 S T を参照している場合には、設定前に定義内容が存在するため、特定内容を設定するとともに設定前の定義内容をガイダンス表示して比較しながら対話的に設定内容をドキュメント編集処理部 2 0 9 により修正する。

【 0 0 6 3 】

P P 作成の場合は本動作をスキップして以降の根拠マトリクス生成ステップ 3 1 0 に移る。

【 0 0 6 4 】

ステップ 3 1 0 :

ツールメニュー 6 0 1 の根拠マトリックス生成・検証 6 0 9 選択により、根拠マトリックス生成・検証処理部 2 1 6 が、3 章～6 章（P P 作成の場合 5 章）までの環境—目標—C C 要件—実現方式の対応関係から各項目間の対応マトリックス表を自動生成、未対応情報の有無を検証して有の場合はメッセージ通知し、ドキュメント編集処理部 2 0 9 により対話的に修正する。

【0065】

ステップ311:

ツールメニュー601のPP/ST簡易評価610において、PPの場合はPP簡易評価611、STの場合はST簡易評価612選択により、PP/ST簡易評価処理部217がCC (CEM) /PKG構造化DB202を検索してCEMのPP/ST評価チェックリストを問診表形式でダイアログ表示し、対話的に各チェック項目のOK/NGチェックボックスをマウス222入力することで作成PP/STの簡易評価をする。

【0066】

ステップ312:

ファイルメニュー613の名前を付けて保存選択、名称設定し、作成PP/STを事例・ノウハウ情報管理制御部208によりローカルPP/ST構造化DB203に登録する。

【0067】

本実施例によれば、以下の効果がある。

【0068】

・登録PPや過去のPP/ST作成事例やその部分を画面上PP/ST間の継承関係に基づきツリー表示される事例PP/STアイコンから設計対象に参照すべき適切なPP/STを容易に選択できる。これを雛型や部品として再利用あるいは参照情報として活用することで、CCや脅威・対策、リスク分析の専門知識・ノウハウや技術を持たない設計者でもPP/STの作成可能となる。

【0069】

・原案自動生成と追加修正による準自動作成により作成工数の効率化や作成品質の均一化が図れるCC準拠のセキュリティシステム設計支援が実現できる。

【0070】

・最適目標決定手段により投資効果の良いPP/ST作成ができ、PP/ST簡易評価手段による自己評価により正式の評価機関による評価の手戻りを少なくし、評価コストも削減することができる。

【0071】

・作成PP/STや作成過程の情報をデータベース格納する手段により、ツール利用しながら雛型事例や事例部品の拡張・充実を図ることができる。

【0072】

次に本発明の第二実施例を説明する。本実施例は、図10にシステム構成図を示すように、ネットワーク接続形態でセキュリティシステム設計支援サービスを提供する場合の例である。システム動作は、第一実施例の場合と同様である。図10に示す構成における特徴点は以下の通り。

【0073】

・設計支援サービスサーバ901を設け、サーバ内のデータベース902に図2のデータベース206と同じ事例/ノウハウ情報を格納する。

【0074】

・サーバ内のプログラムメモリ903に図2のプログラムメモリ219と同じ設計支援処理プログラム群を格納して複数利用者間で共有する。

【0075】

以上のような構成により、各利用者は、自身のクライアント225より、ネットワークインターフェース904、905でネットワーク906を介して設計支援サービスサーバ901にアクセスする。サーバ内のプログラムメモリ903からクライアント225のプログラムメモリ219への設計支援処理プログラム群のダウンロード、あるいはプログラムメモリ903の設計支援処理プログラム群へのリモートアクセスにより、サーバ側のCPU907、ワークメモリ908を活用する。これらの操作によりデータベース902上の事例/ノウハウ情報を検索・照会することでPP/ST作成支援を実現する。

【0076】

本実施例によれば、登録及び過去のPP/ST作成事例や部品情報を共有化して再利用・有効活用することができる。またサーバ管理とすることで利用者側の情報更新負荷をかけず、最新情報を活用することができる。

【0077】

さらにネットワーク接続で利用できることにより、利用場所に制約されずPP

／ST作成支援サービスを提供することができる。

【0078】

次に本発明の第三実施例を説明する。本実施例は、図11にシステム構成図を示すように、水平分散ネットワーク接続形態でセキュリティシステム設計支援サービスを提供する場合の例である。システム動作は、第一、第二実施例と同様である。図11に示す構成における特徴点は以下の通り。

【0079】

- ・組織毎に複数の設計支援サービスサーバ1001、1002を設ける。

【0080】

- ・サーバ内のプログラムメモリ903に分散DBリンク制御部1003、1004を設ける。分散DBリンク制御部1003、1004により、複数組織の事例／ノウハウDBをネットワーク906を介して仮想的な統一DBとして事例／ノウハウ情報を検索・照会することでPP／ST作成の支援を実現する。

【0081】

本実施例によれば、各組織毎の登録及び過去のPP／ST作成事例や部品情報を共有化して再利用・有効活用することができる。またこれにより提供情報の充実が図られ、特定組織グループや業界としてPP／ST作成の均一化も図ることができる。

【0082】

次に本発明の第四実施例を説明する。本実施例は、図12にシステム構成図を示すように、金融関係情報システムに関して垂直分散ネットワーク型でセキュリティシステム設計支援サービスを提供する場合の例である。システム動作は、第一ないし第三実施例と同様である。図12に示す構成における特徴点は以下の通り。

【0083】

- ・民間金融機関に設計支援サービスサーバ1101、国内公的金融管理機関に基準提供サーバ1102、国際PP登録機関に国際基準提供サーバ1103を設ける。

【0084】

・国際PP登録機関基準提供サーバ1103のデータベース1104内には、登録PP/PPファミリー構造化DBとCC（CEM）/PKG構造化DBを格納する。

【0085】

・国内公的金融管理機関基準提供サーバ1102のデータベース1105には、ATMや銀行決済システム、インターネットバンキングシステムなどの国内金融系システムに特化して作成・登録された金融系国内登録PP/PPファミリー構造化DB、ローカルPP/ST構造化DB、拡張CC/PKG構造化DBを格納する。

【0086】

・民間金融機関設計支援サービスサーバ1101のプログラムメモリに情報更新監視制御部1106を設ける。

【0087】

情報更新監視制御部1106は、国際機関1103、国内機関サーバ1102の情報更新を監視し、更新検知時には民間機関サーバ1101へ情報をダウンロードする。また国際機関、国内金融機関の階層レベルや適用分野特化の異なる事例情報をネットワーク906を介して検索・照会することでPP/ST作成の支援を実現する。

【0088】

本実施例によれば、各機関毎に登録及び適用分野特化のPP/ST作成事例や部品情報を管理することで、情報の管理負荷を軽減でき、最新の情報を提供することができる。また適用分野に特化した情報共有化により、特定分野の利用者に対してより適した有効な情報提供を図ることができる。

【0089】

次に本発明の第5の実施例としてPP/ST作成のための事例/ノウハウ情報を携帯して利用する場合について、図13を用いて説明する。

【0090】

図13は、携帯事例利用型のセキュリティシステム設計支援ツールの構成図で

ある。

【0091】

システム動作は、第一、第二実施例の場合と同様である。図13に示す構成における特徴点は以下の通り。

【0092】

・ ツールのデータベース206に格納されるPP/ST関連事例/ノウハウ情報を図13に示す事例/ノウハウデータベースフロッピーディスク1201または事例/ノウハウデータベースCD-ROM1202などの可搬型記憶媒体に登録する。

【0093】

これにより、事例/ノウハウデータベース情報を携帯し、フロッピーディスクドライバ1203またはCD-ROMドライバ1204を内蔵したセキュリティシステム設計支援ツール上で事例情報を照会し、PP/ST作成の支援を実現する。

【0094】

本実施例によれば、顧客先等の移動先でのPP/ST作成やシステム設計コンサルテーションをする際にも、フロッピーディスクドライバまたはCD-ROMドライバを内蔵したノート型パーソナルコンピュータ上のセキュリティシステム設計支援ツールを用いて事例/ノウハウデータベース情報を有効活用することができ、質の高い提案やコンサルテーションサービスを提供することができる。

【0095】

【発明の効果】

本発明によれば、ある基準に基づく情報システムの計画・設計段階における要求仕様書や基本設計書の作成作業において、登録された仕様書や過去の作成事例やその部分を雛型や部品として再利用あるいは参照情報として有効活用できる。

【0096】

したがって、専門知識・ノウハウや技術を持たない設計者でも要求仕様書や基本設計書の作成が可能となる。さらに、かつ作成工数の大幅な効率化や作成品質の均一化を可能とする設計支援が実現できる。

【0097】

またコストを考慮した最適な目標を設定した要求仕様書や基本設計書を作成できることから、高い投資効果が期待できる。

【図面の簡単な説明】

【図1】

本発明に基づくセキュリティシステム設計支援ツールの特徴概要図である。

【図2】

セキュリティシステム設計支援ツールの構成図である。

【図3】

PP/ST作成処理の動作フロー図である。

【図4】

PP/ST作成処理の動作フロー図である。

【図5】

PP/STテンプレート設定画面の一実施例を表す図である。

【図6】

PP/STDキュメント編集画面の一実施例を表す図である。

【図7】

ツールメニュー選択画面の一実施例を表す図である。

【図8】

対応ノウハウデータベースの構成図である。

【図9】

条件・評価関数指定画面の一実施例を表す図である。

【図10】

ネットワーク型セキュリティ設計支援システムの構成図である。

【図11】

水平分散ネットワーク型セキュリティ設計支援システムの構成図である。

【図12】

垂直分散ネットワーク型セキュリティ設計支援システムの構成図である。

【図 1 3】

携帯事例利用型セキュリティ設計支援ツールの構成図である。

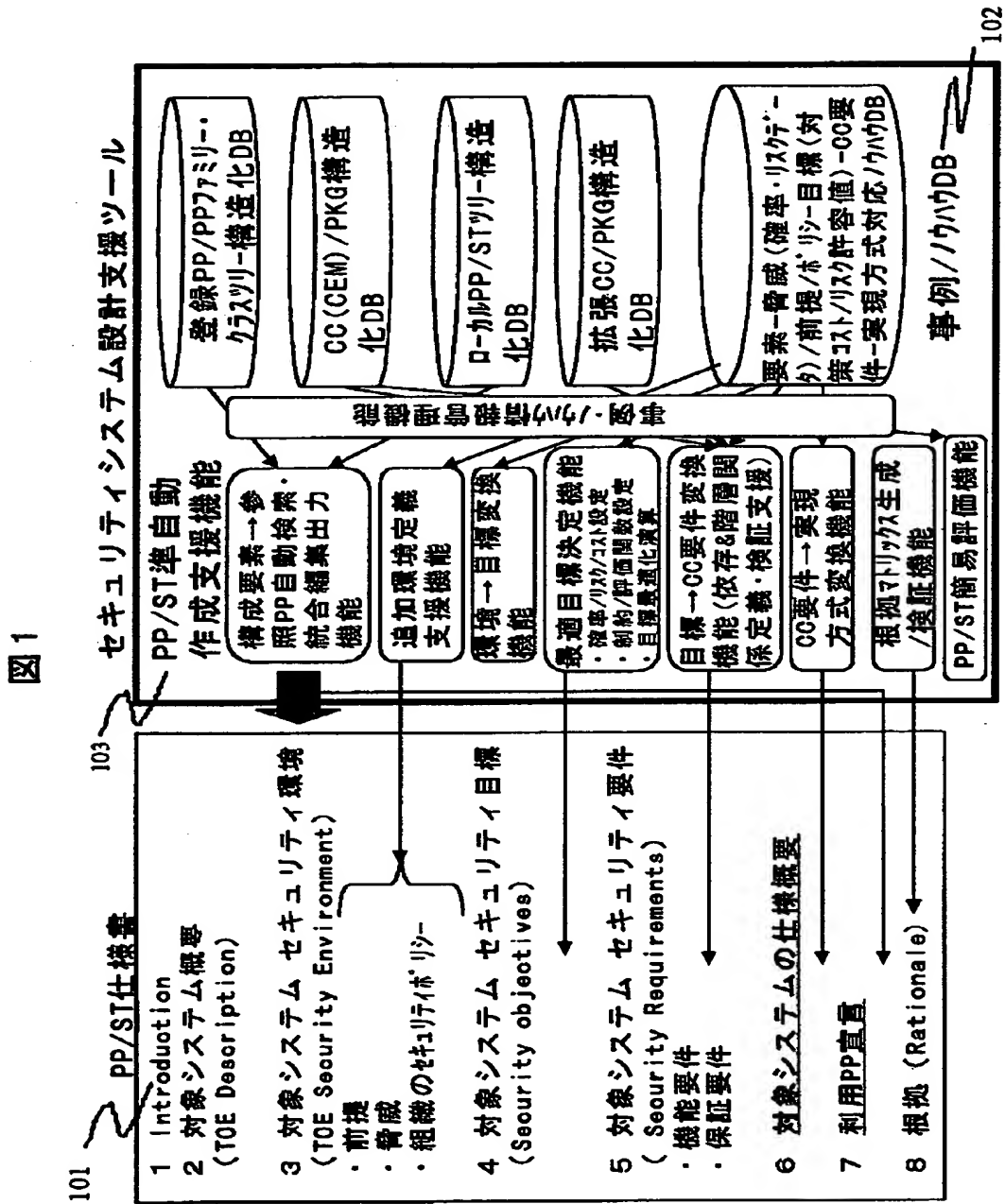
【符号の説明】

1 0 1 … PP / ST仕様書, 1 0 2 … 事例 / ノウハウデータベース, 1 0 3  
… PP / ST準自動作成支援機能。



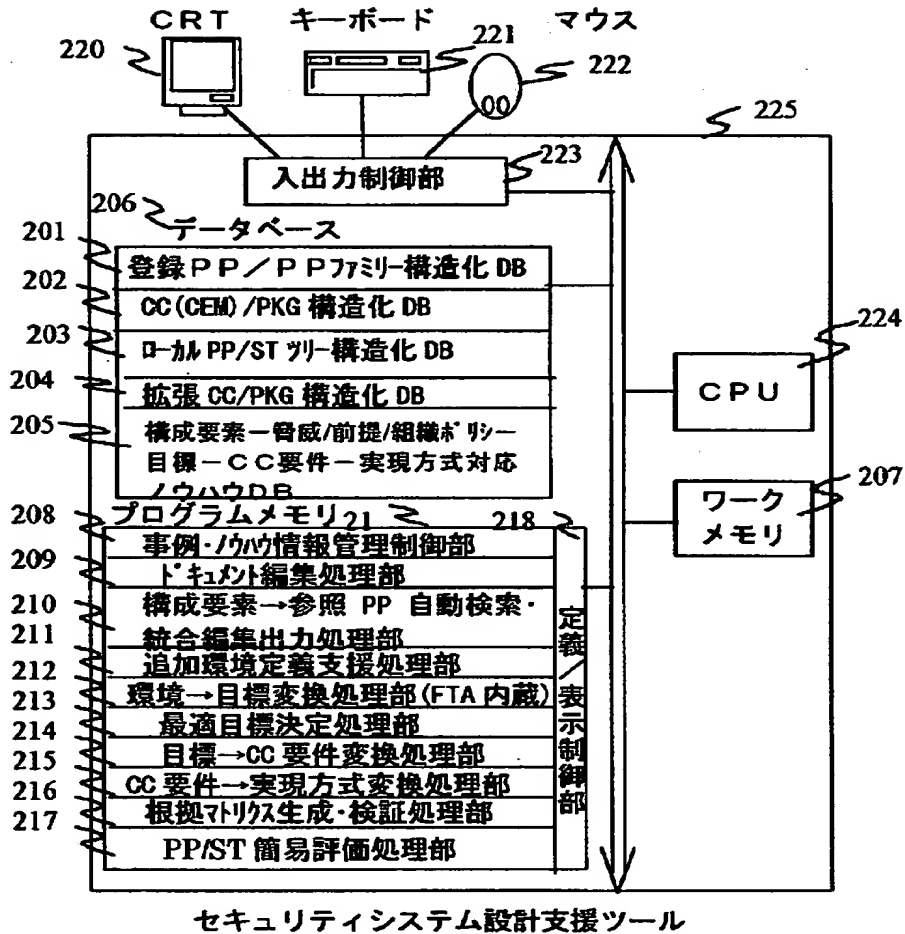
【書類名】 図面

【図 1】



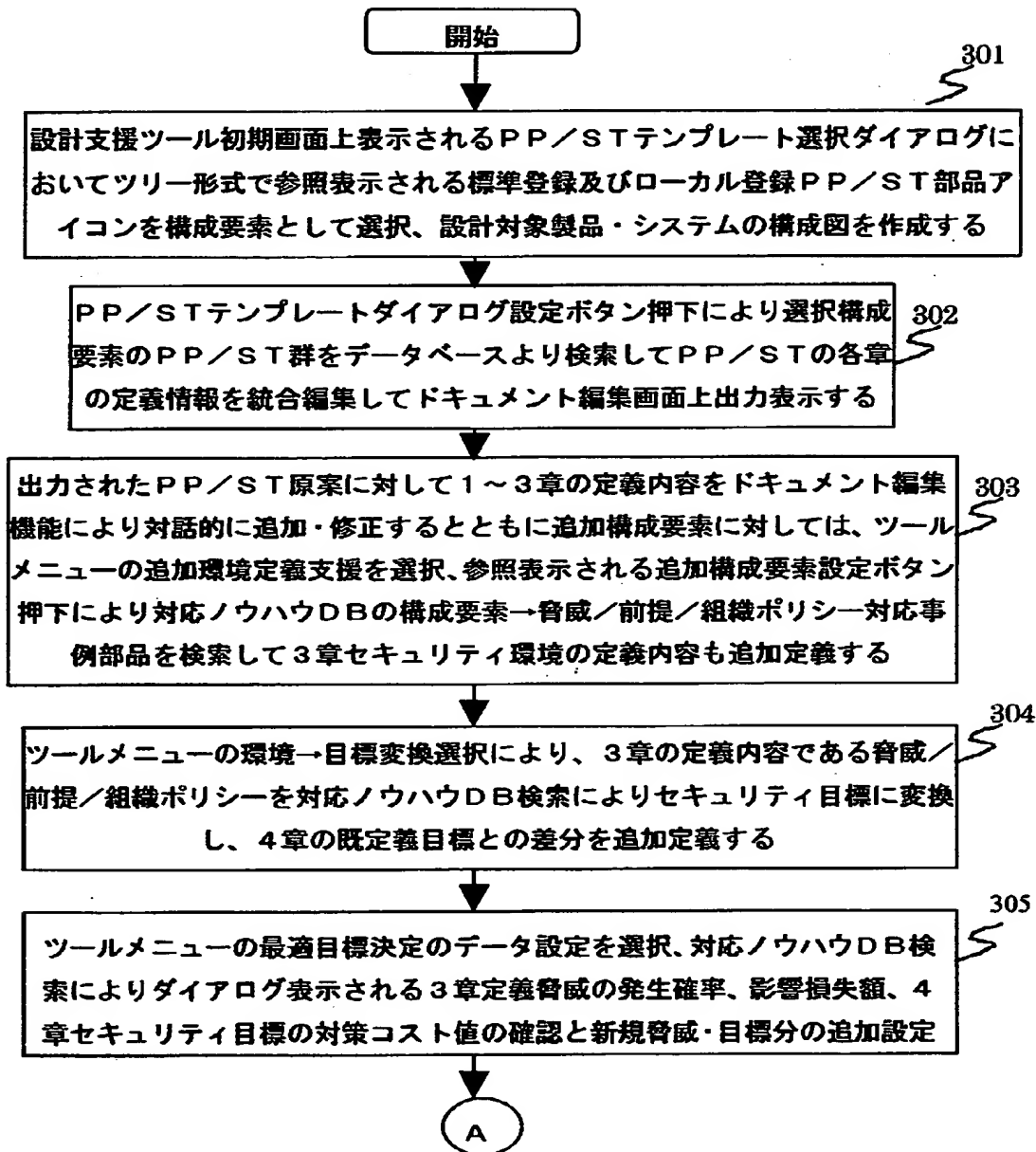
【図 2】

図 2



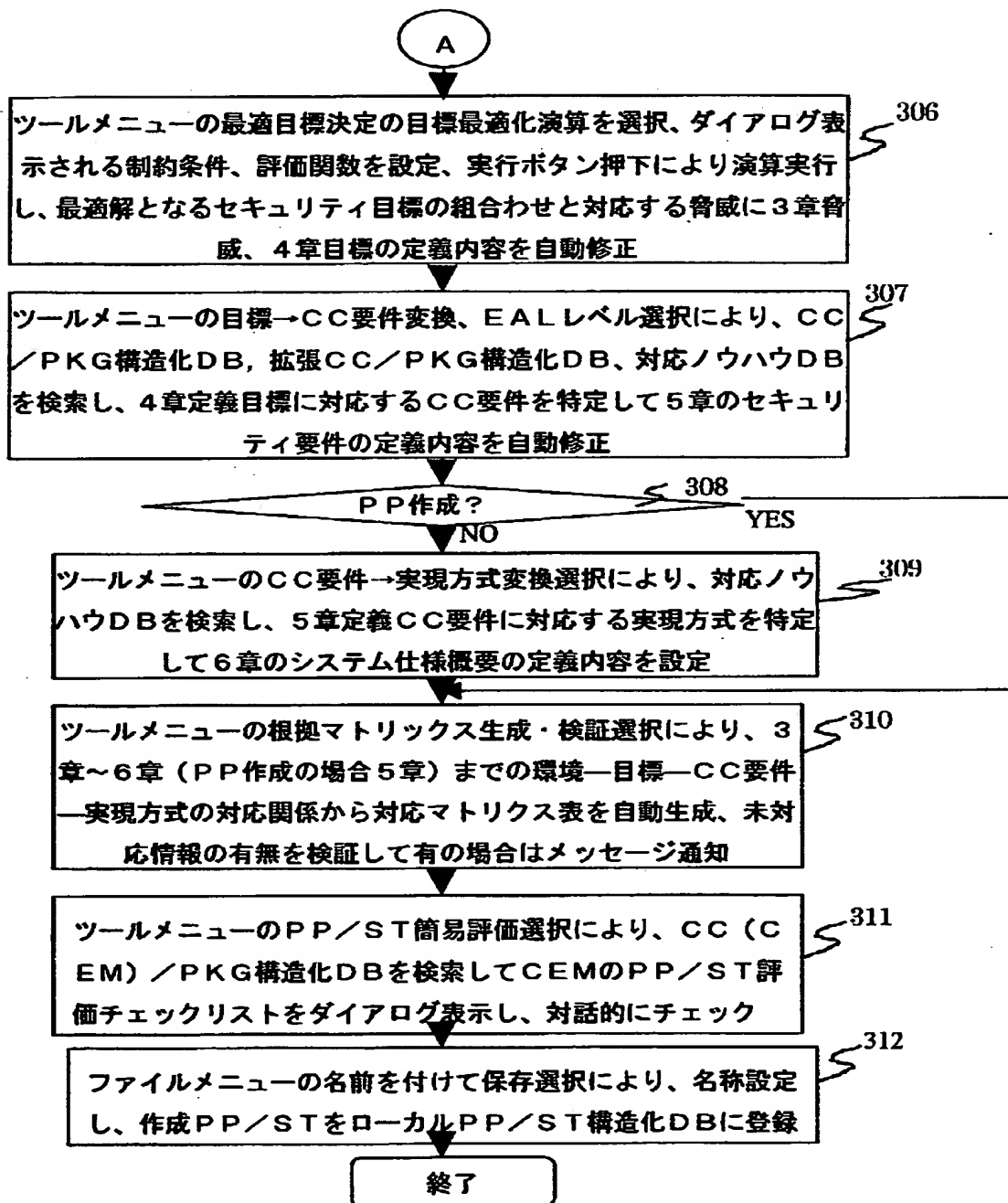
【図 3】

図 3

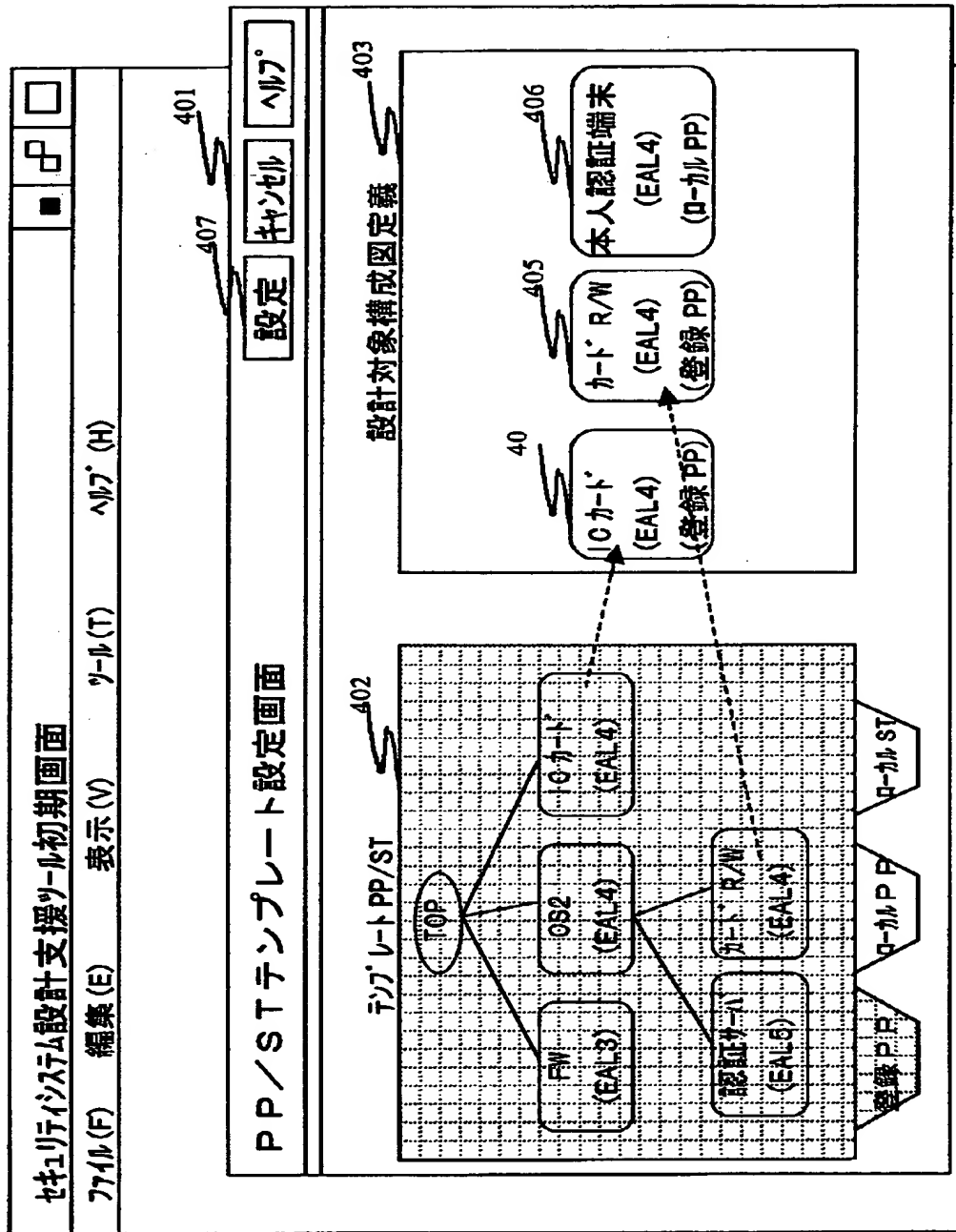


【図 4】

図 4



【図 5】



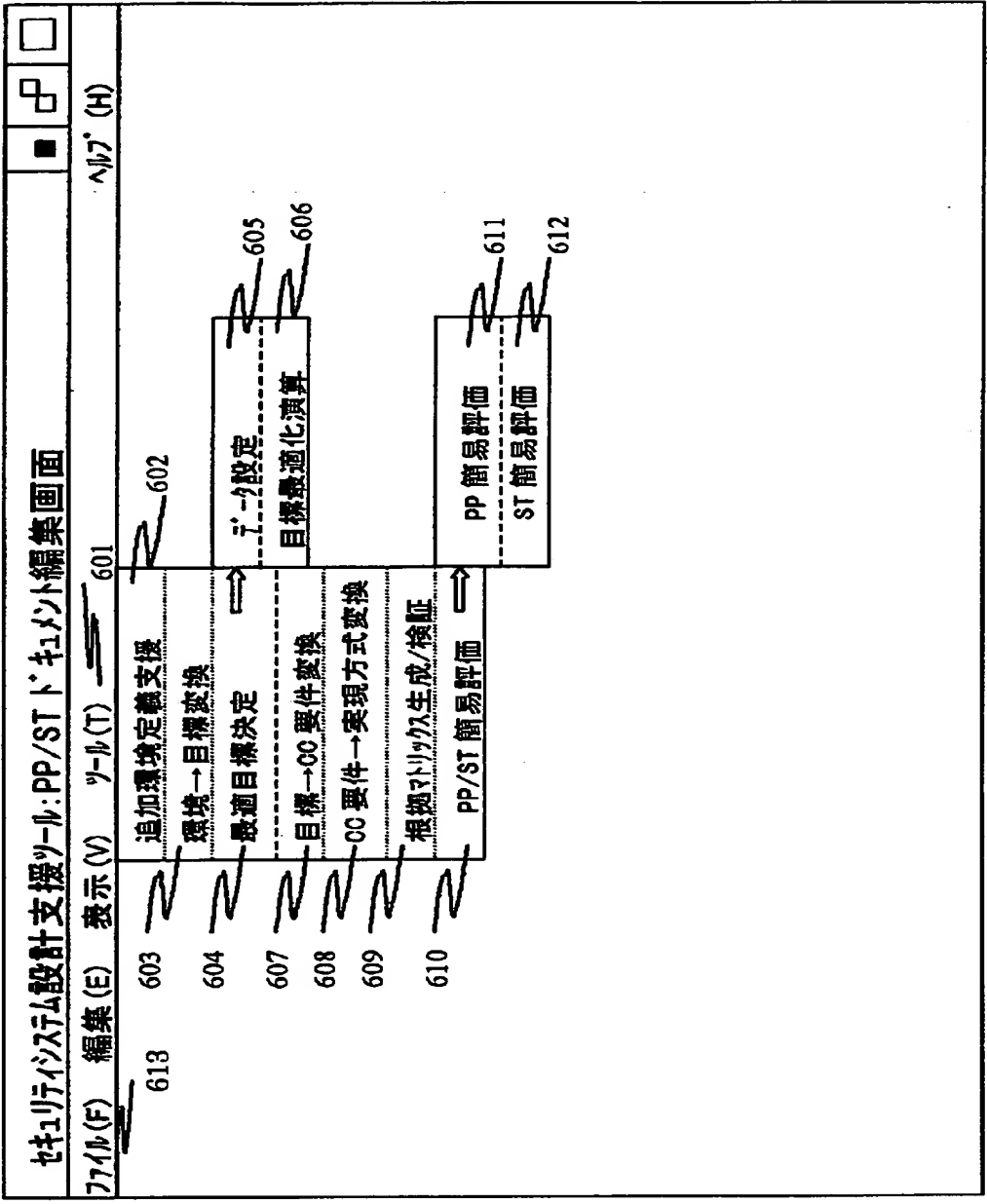
【図 6】

図 6

セキュリティシステム設計支援ツール:PP/STドキュメント編集画面					501	■	□
ファイル(F)	編集(E)	表示(V)	ツール(T)	ヘルプ(H)			
1 章 : はじめに							
ICC-PP ; はじめに		502					
R/W-PP ; はじめに							
端末-PP ; はじめに							
2 章 : 対象システム概要							
ICC-PP ; システム概要		503					
R/W-PP ; システム概要							
端末-PP ; システム概要							
3 章 : セキュリティ環境							
3. 1 前提							
ICC-PP ; 前提							
R/W-PP ; 前提							
端末-PP ; 前提							
3. 2 脅威							
7 章 : 利用PP宣言							
504							
ICC-PP識別名							
R/W-PP識別名							
8 章 : 根拠							

【図 7】

図 7



【図 8】

図 8

701 構成要素・環境対応表

要素	前提	脅威	組織ポリシー
CompX	A.XXX	T.XXX	P.XXX
...	...	...	...

702 環境・目標対応表

環境	目標
A.XXX	O.AXX, O.AYY, O.AZZZ
...	...
P.XXX	O.PXX, O.PYY
...	...
T.XXX	(O.TXX, O.TYY), (O.TZZ)
...	...

704 脅威子一覧表

脅威	発生確率	影響損失額 (¥)
T.XXX	0.004	1000,000
...	...	...

705

対策コスト子一覧表

対策 (目標)	対策コスト (¥)
O.TXX	10,000
...	...

706

目標・CC要件対応表

目標	CC機能要件
O.TXX	FAU_GEN.1, FAU_STG.1
...	...

707

CC要件・実現方式対応表

CC機能要件	実現方式
FAU_GEN.1	ImpX
...	...



【図 9】

図 9

セキュリティシステム設計支援ツール:PP/STドキュメント編集画面			<input type="checkbox"/>	
ファイル(F)	編集(E)	表示(V)	ツール(T)	ヘルプ(H)

801

804

実行

キャンセル

ヘルプ

目標最適化条件・評価関数指定

評価関数指定 ; 802

コスト最小化関数	<input checked="" type="checkbox"/>
コスト最小化関数	<input type="checkbox"/>
対策リスク最大化関数	<input type="checkbox"/>

制約条件・値指定 ; 803

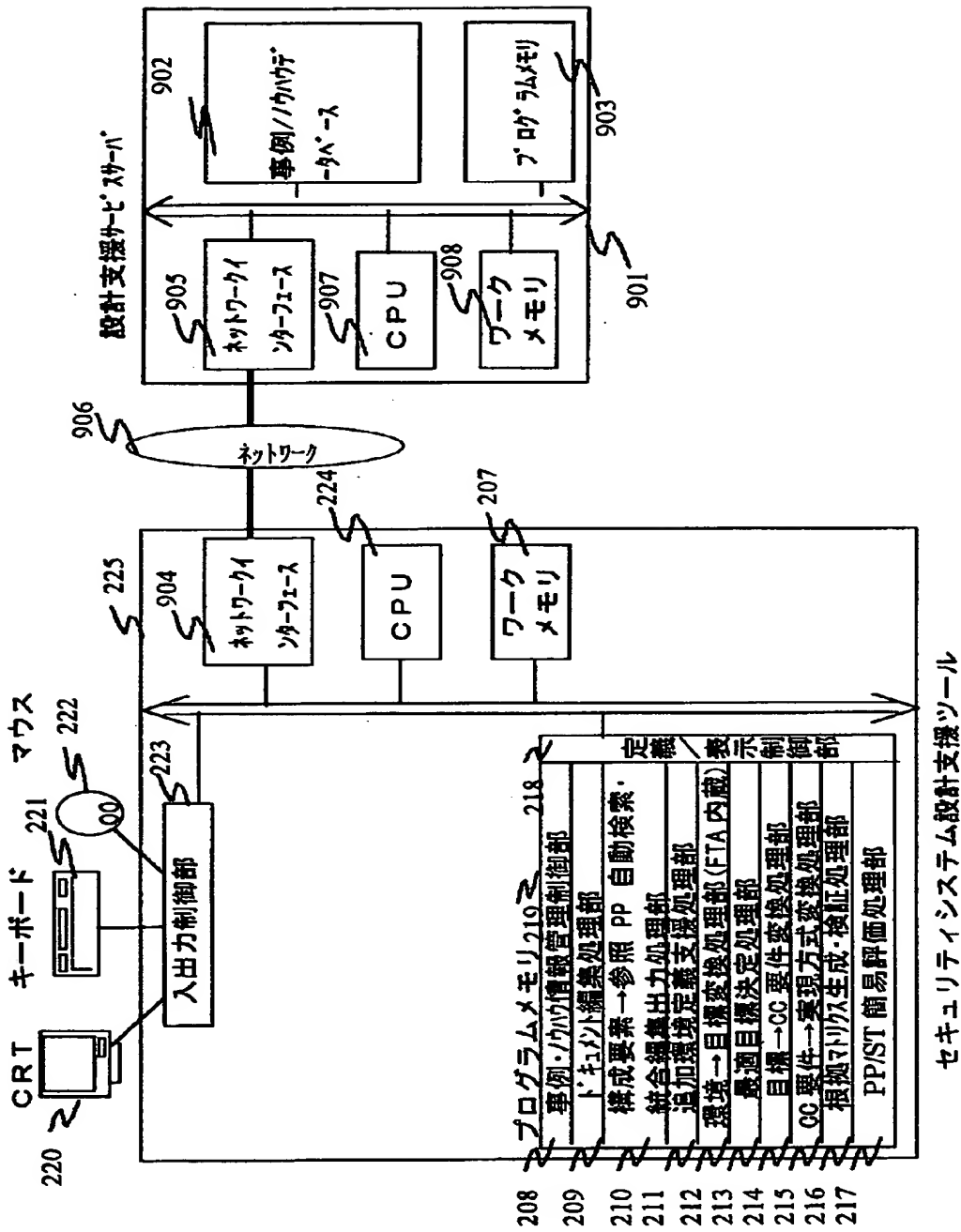
☒ リスク許容値 : ¥ 100,000

☐ コスト制限値 : ¥

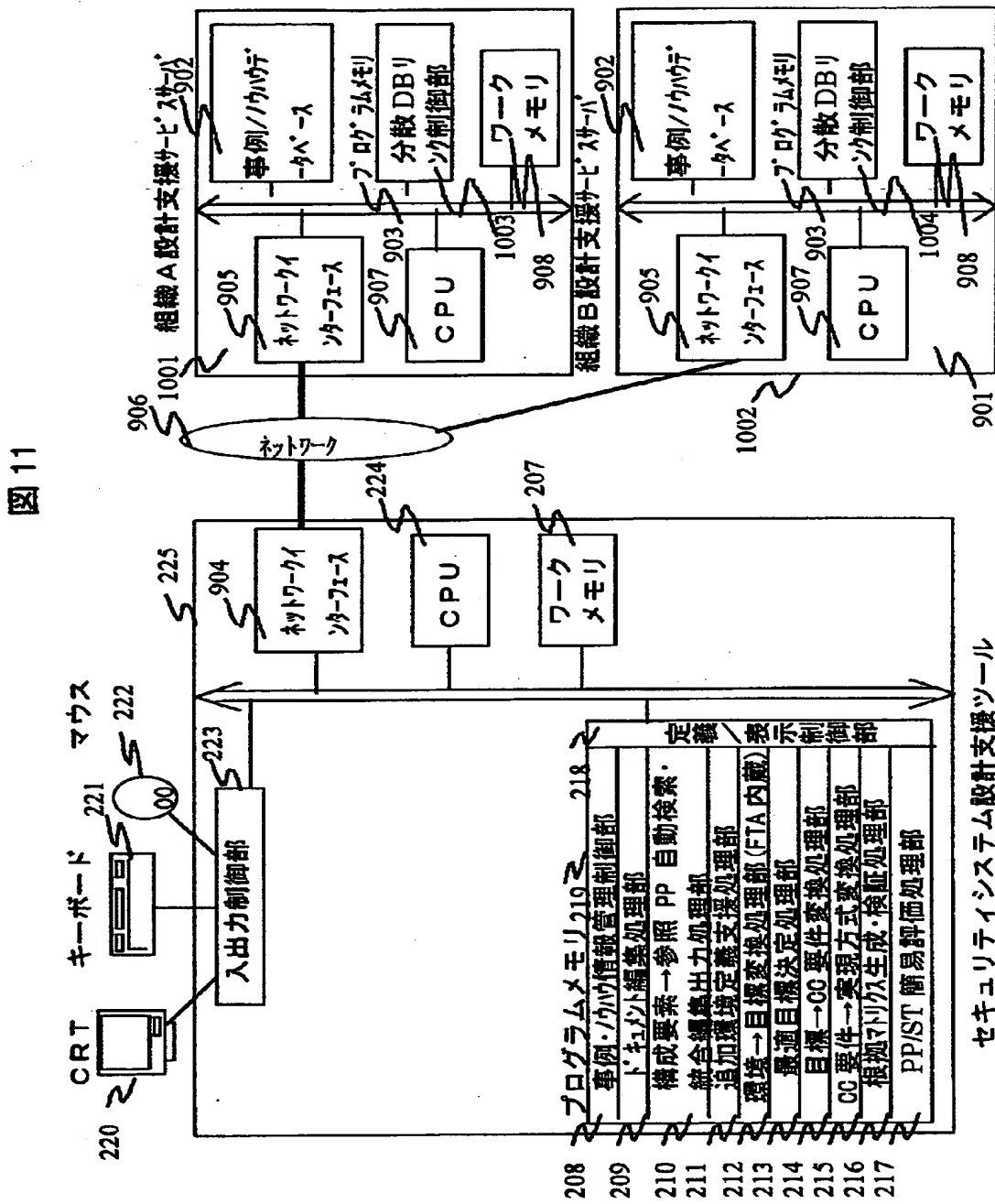
☐ リスク対コスト比率 :

【図10】

図10

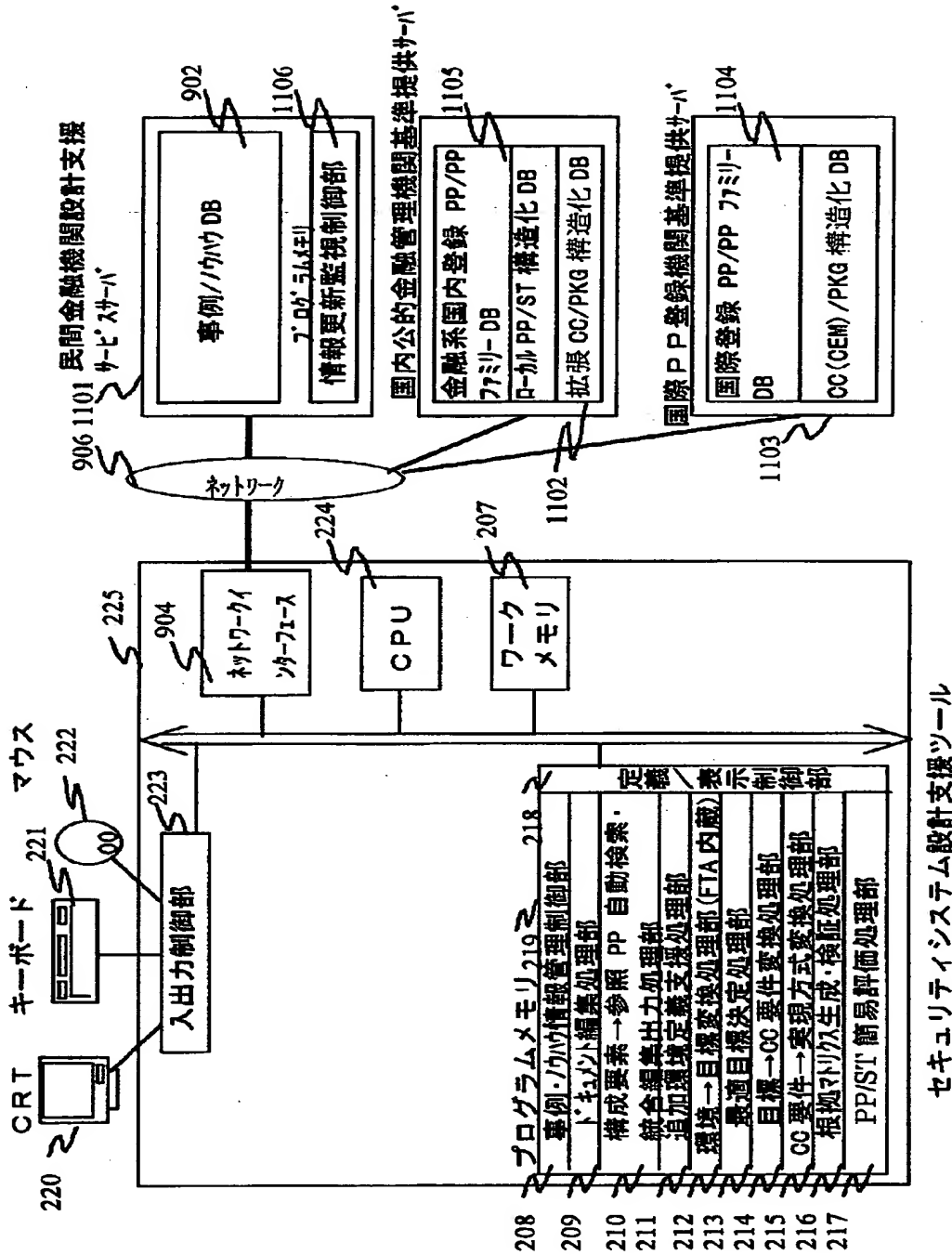


【図 11】

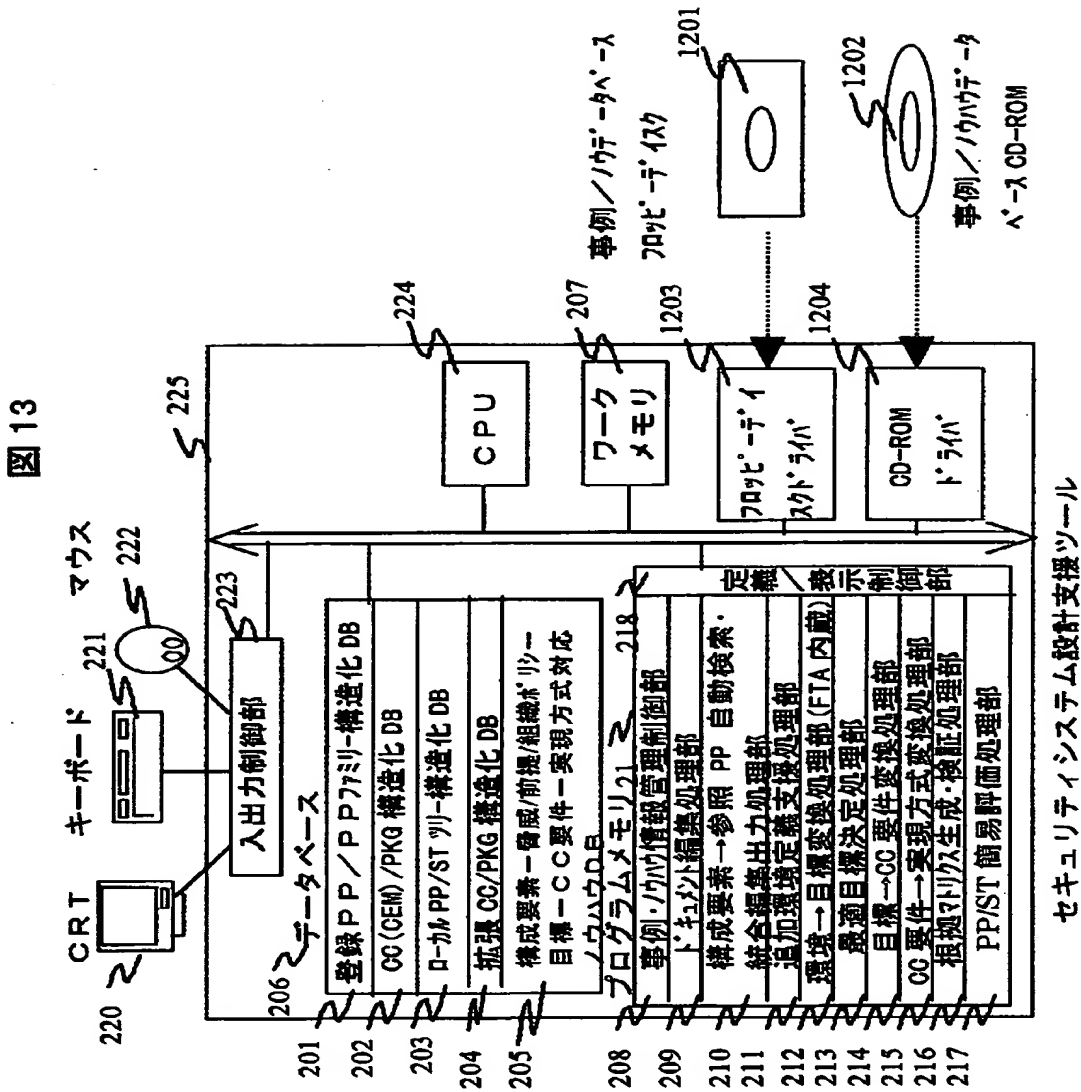


【図 1 2】

図 12



【図 1 3】



【書類名】 要約書

【要約】

【課題】

セキュリティ評価基準に準拠した製品やシステムの設計時におけるセキュリティ要求仕様書やセキュリティ基本設計書作成を、専門家でない一般の設計者でも効率化、均一化できるようにするツール及び方法を提供する

【解決手段】

登録 P P や過去の P P / S T 作成事例を雛型として再利用、参照できるよう構造化し、原案を自動生成する手段と、過去の作成事例やその過程で蓄積した部分事例データベースを活用し、部分自動生成による追加・修正手段とを持たせる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所